IN THE UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**NO. 3:21-cr-00236**
v.	)	
	)	**JUDGE CAMPBELL**
MATTHEW LYNCH	)	

FINDINGS OF FACT, CONCLUSIONS OF LAW, AND VERDICT

This matter came before the Court for a bench trial. At the conclusion of the trial, the Court took the matter under advisement for deliberation and decision. At the request of Defendant, the Court provides its written decision pursuant to Federal Rule of Criminal Procedure 23(c).

I. PROCEDURAL HISTORY

On February 5, 2025, a federal grand jury returned a Superseding Indictment (Doc. No. 106) against Defendant Matthew Lynch:[1]

COUNT ONE

THE GRAND JURY CHARGES:

> Beginning on a date unknown to the Grand Jury, but no later than April 11, 2017, in the Middle District of Tennessee, the defendant, **MATTHEW LYNCH**, knowingly received any visual depiction using any means and facility of interstate or foreign commerce and that had been shipped and transported in and affecting interstate or foreign commerce, by any means including by computer; and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.
>
> In violation of Title 18, United States Code, Sections 2252(a)(2) and (b).

[1] The Superseding Indictment expanded the timeframe of Count One. (*Compare* Doc. No. 3 *with* Doc. No. 106). In the original Indictment returned October 13, 2021, the timeframe of Count One was "[b]eginning no later than October 13, 2016, through on or about April 11, 2017." The charges are otherwise the same.

COUNT TWO

THE GRAND JURY FURTHER CHARGES:

> On or about October 29, 2016, in the Middle District of Tennessee, the defendant, **MATTHEW LYNCH**, did knowingly possess or access with intent to view at least one matter which contains any visual depiction that had been shipped and transported in and affecting interstate and foreign commerce and was produced using materials which had been mailed and shipped and transported using any means and facility of interstate and foreign commerce, including by computer, the production of such visual depiction involved the use of a prepubescent minor who had not attained 12 years of age engaging in sexually explicit conduct, and such visual depiction was of such conduct.
>
> In violation of Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2).

(Superseding Indictment, Doc. No. 106).

Defendant waived his right to a jury trial on December 10, 2024. (Doc. No. 90). The Government consented (*see* Doc. No. 86), and the Court granted the motion for the case to be tried by the Court (Doc. No. 91). The bench trial commenced on April 15, 2025, and concluded on April 17, 2025, and the Court took the matter under advisement. Having considered the testimony, exhibits, and all the evidence admitted at trial, the Court hereby renders its verdict, and in accordance with Federal Rule of Criminal Procedure 23(c), sets forth the following specific finding of fact and conclusions of law.

II. LEGAL STANDARD

The Government has the burden to prove each element of the alleged offenses beyond a reasonable doubt. Of course, proof beyond a reasonable doubt does not mean proof beyond all possible doubt. Reasonable doubt must be based on reason and common sense. Doubt based on pure speculation is not reasonable.

In assessing the credibility or believability of witnesses, the Court as the factfinder

considers a number of factors including: how the witness acted while testifying, potential bias, the consistency of the testimony, and the believability of the testimony in light of all of the other evidence. With regard to expert testimony, the Court also considers the experts' background and qualifications and how they reached their conclusions.

III. FINDINGS OF FACT

A. The Government's Proof

1. Witnesses

Four witnesses testified on behalf of the Government.

Robert Carrigan was an investigating officer on this case. Until his retirement in 2023, Carrigan worked for the Metropolitan Nashville Police Department ("MNPD") for over thirty years. He served as a detective on the Internet Crimes Against Children Task Force from 2001 until 2023. Ninety percent of his caseload involved internet-related child sexual abuse material ("CSAM") cases.

Chad Gish testified as an expert in the area of digital forensics. Gish worked for MNPD for over twenty-six years. He was involved in starting the MNPD digital forensics laboratory and worked as the lab manager for almost twenty years until he retired from full-time work for MNPD in 2024. He continues to work for MNPD on a part-time basis doing quality-control and training. Gish has over 4,000 hours in digital forensics training and has testified as an expert in digital forensics over 200 times.

David Thomas also testified as an expert in the area of digital forensics. Thomas has over ten years' experience as a computer forensic analyst. His work on this case was in his capacity as a computer forensic analyst for Homeland Security Investigation, where he was employed from 2017-2023. He has worked on over one hundred investigations involving CSAM.

Savannah Debraux is a Special Agent for Homeland Security Investigation ("HSI") in the child exploitation and human trafficking group. She is the case agent assigned to the investigation of the Defendant.

During the trial, the Court heard the testimony of these witnesses and observed their demeanor while testifying. Each of these witnesses is well-qualified in their areas of expertise. Although they are witnesses for the Government, the Court does not find that bias affected their testimony. Overall, their testimony was consistent and believable in light of other evidence presented. Their demeanor while testifying leads the Court to believe that the testimony provided was honest and forthright to the best of the witnesses' ability. In summary, the Court finds the testimony of these witnesses to be credible. These findings of fact reflect this credibility determination.

2. Pinterest Image

On December 14, 2016, the National Center for Missing and Exploited Children ("NCMEC") received a report from Pinterest Inc. concerning an incident categorized for purposes of the report as "Child Pornography (possession, manufacture, and distribution)." (Gov't Ex. 5). Detective Carrigan testified that NCMEC is an organization established by Congress to act as a clearinghouse for reporting child exploitation materials. NCMEC receives reports of suspected child exploitation, determines the likely jurisdiction of the offender, and then forwards the information to local law enforcement in that jurisdiction for investigation. NCMEC also maintains a database of material submitted to them and cross-references submitted images to identify known victims and connections to other incidents involving the same images. Electronic service providers are required by law to submit information to NCMEC if they find child exploitation material on their networks.

The Government provided evidence through the testimony of Savannah Debraux that Pinterest is a website or mobile application that users can use to search for images and then "pin" or "repin" them to the user's "board." Similar to bookmarking a file or a link, "pinning" allows the user to review the image at a later time. The user's "board" is a collection of those pinned images.

Pinterest is an electronic service provider and is, therefore, required to report suspected CSAM to NCMEC. As relevant here, Pinterest submitted information to NCMEC that, on October 29, 2016, a user named "Matt Matt" with a verified email address of mattlynch6262@gmail.com pinned or repinned the reported image from a Pinterest board named "BoobiesBoard" via "IN_APP_BROWSER". Detective Carrigan testified that a "verified email address" is one that the user verifies during the registration process by responding to an email from the service provider. That the image was "repinned" using an "in-app browser" means the user "clicked through a Pin to view the original website, then pinned the image from within the browser preview." (*See* Gov't Ex. 5, Def. Ex. 8).

The NCMEC report and information later obtained from Pinterest shows that all the reported activity by the user was from IP address 107.142.100.65. (Gov't Exs. 3, 5). It was from this IP address that the user registered the account, logged in on multiple occasions, and pinned or repinned the reported image. (*Id*.). The Government submitted evidence showing that Defendant had an AT&T U-verse account that was assigned the unique IP address 107.142.100.65 with a service address corresponding to Defendant's home address. (Gov't Ex. 1).

NCMEC sent the report, including the reported image, to the MNPD, which received the report on February 1, 2017. The image shows three young girls sticking out their tongues and pinching their nipples. The photo shows the genitals or pubic area of the girls. A pink object that

appears to be a toy is partially covering the pubic area of one of the girls. The size and body development of the girls indicates that they are minors; at least two of the girls are prepubescent and under the age of twelve.

Based on the NCMEC report and subsequent investigation, investigators obtained a search warrant for Defendant's apartment. When investigators executed the search warrant on April 11, 2017, Defendant told them that mattlynch6262@gmail.com was his Gmail account, that he had a Pinterest account, and that he was locked out of Pinterest account "a few months ago" and that he had been locked out of Pinterest on at least one other occasion. (Gov't Exs. 6, 6A).

Pursuant to the search warrant, investigators seized a Dell Laptop, a Maxtor hard drive, and two cell phones from Defendant's apartment. The image reported by Pinterest did not appear on any of these devices. Investigators did, however, find other images.

3. Laptop

During the execution of the search warrant, Defendant told investigating officers the laptop was his personal laptop, it was password protected, and that he purchased it new approximate a year before the execution of the search warrant. (Gov't Exs. 6, 6A). Two forensic extractions were performed on the laptop. The first was performed in 2017 by Chad Gish of the Metropolitan Nashville Police Department, Computer Forensics Section. (Gov't Ex. 17). In 2023, a second extraction using more advanced software than was available in 2017 was performed by David Thomas of Department of Homeland Security Investigations. (Gov't Ex. 52). Gish and Thomas testified as experts in computer forensics. They explained the process for extracting data, indicators of reliability of the extraction, how and where the data is stored on a device, and discussed the data recovered from each of the devices.

Gish and Thomas testified that the only user account on the laptop was that of the

Defendant. The laptop had evidence of other accounts associated with Defendant, including email and Skype accounts, and contained personal photos of Defendant. (*See* Gov't Exs. 57-60). Gish and Thomas testified that the laptop did not contain evidence of accounts belonging to anyone other than Matthew Lynch, and the forensic examiners found no evidence of anyone other than Matthew Lynch using the laptop.

More than one thousand images categorized by investigators as CSAM were recovered from the laptop. Most of these were in "unallocated" space, meaning they had once been stored on the laptop or accessed from the laptop, but were no longer active files. Files from unallocated space cannot be viewed without forensic software. In contrast, files in "allocated" space are active files. More than twenty images recovered from the laptop were admitted into evidence. (Gov't Exs. 28, 29, 30, 31, 71A-71K; 72A-72I). The images in Government Exhibits 28-31 and 71A-71K were recovered from the allocated space on the laptop. The remaining images were found in unallocated space.

Several images in allocated space on the laptop were in a folder associated with a software program installed on the laptop called FrostWire. (Gov't Exs. 28, 29, 30, 31). Detective Gish testified that FrostWire is a peer-to-peer file sharing program that allows a user to access anonymous file sharing network to download torrent files, and that the torrent network is known for hosting child sexual abuse material and child exploitation material. Detective Gish explained that to download material from the torrent network, a user must search for requested files and then double click to select the specific file from the search results to download the material.

The FrostWire folder on Defendant's laptop contained a compression file named *[April_2014][ALLTIMENUDES]1St Studio-Siberian Mouse-Nk007 Sample (Pthc 2012 Pedo).rar*. (Gov't Ex. 27; Gish Rept., Gov't Ex. 17 at 15). A compression file contains compressed data that

takes less space and can be downloaded more quickly. Detective Gish testified that "Siberian Mouse" is a well-known CSAM series. "PTHC" is an abbreviation for "Preteen Hard Core," a term used to describe CSAM materials depicting very young children being subjected to rape and other abuse. The "Siberian Mouse" compressed file contained four image files. (Gov't Exs. 28-31).

Three of the images appear to be advertisements. (Gov't Exs. 28-30).

Government Exhibit 28 is a collage or image with many other images within it. Most of the images within the collage are of minors engaging in sexually explicit conduct. By way of example, the image in the lower left-hand corner is a photo with two little girls on a bed with teddy bears; their legs are spread apart, and their vaginas are exposed; based on their body development (lack of body hair, breast development, hips), the girls are prepubescent. The image in the fourth row on the far left is of a very young girl; her legs are spread, her vagina is exposed, and someone is spreading the child's vagina apart with their fingers.

Government Exhibit 29 is an image of two young girls kissing; their breasts are exposed.[2]

Government Exhibit 30 is an image of a young girl. Based upon her size and development, she is a minor. She is entirely nude and is spreading her vagina and touching it with a cylindrical object.

Government Exhibit 31 is what Detective Gish described as a "contact sheet" showing thumbnail images of the contents of a compressed file. The underlying image and video files shown on the contact sheet were not present on the laptop. The hard copy of this exhibit is printed on an 8 ½" x 11" paper. The size of the thumbnail images on this copy makes it difficult to discern the

---

[2] The Government does not contend this image meets the federal definition of CSAM.

age of the subjects from the images themselves, but the sexually explicit nature of the photos is apparent even in the hard copy form. During the trial, however, the image was presented electronically in a larger format in which it was clear that some of these images are of minors engaged in sexually explicit conduct. This finding is consistent with the testimony of Detective Gish, who testified that some of these images depict CSAM, and the file names associated with the images. For example, an image of two young nude boys laying on a bed with their penises exposed has the file name: *[depa][boy+boy]Depa01 2 12Yo Boys Suck Fuck Sound – Pedo G* …[truncated].

All of these files (Gov't Exs. 28-31) were active files in allocated space on the laptop. The files were visible to the user and could be opened and viewed by the user.

The FrostWire folder also included a password protected file named "1St Studio - Siberian Mouse – Nk-007 Sample (Pthc 2012 Pedo).avi*". (Gov't Ex. 32). The file extension type indicates that it is a video file, and the file description suggests it is a video featuring preteens engaged in sexually explicit conduct. But investigators were unable break the encryption to open the file, so the file contents cannot be determined with certainty. There is no evidence that Defendant opened the file.

In addition to the files in the Siberian Mouse folder, Detective Gish testified that forensic artifacts present in the unallocated space of the laptop show that over 1,000 files were transferred from the laptop to a Seagate Go Flex external hard drive and/or were present on the external hard drive and accessed from the laptop. (*See* Gov't Exs. 33, 34, 36-38). These forensic artifacts include: link files, which show the paths of files accessed from the laptop; jump files, which are a kind of internal shortcut for recently accessed files; and thumbnail caches, which show thumbnail images of files in folders that were viewed in thumbnail view. Detective Gish pointed to linked files with

names that suggest that the contents are CSAM images. For example, some of the file names include "PTHC," "jailbait," "pedo," and "kinderficker"; others reference to well-known sets of CSAM images, such as LS Magazine and 1St Studio-Siberian Mouse. Gish testified that the thumbnail images show CSAM material and that some of the thumbnail images are from a well-known series of CSAM material known as LS Island. (*See* Gov't Exs. 36-38).

4. Maxtor Hard Drive

The Maxtor hard drive was found in a storage bin in a closet in Defendant's apartment. Dave Thomas testified that the hard drive is an internal hard drive that had been removed from a desktop computer (not a plug-in external hard drive). The hard drive was in use between approximately 2002 and 2008. When seized from Defendant's apartment, the hard drive was not usable and had to be sent to the HSI laboratory in Virginia to be repaired and extracted. The extracted data showed that defendant and his father had used the hard drive. The Maxtor hard drive contained images categorized as CSAM by investigators in allocated and unallocated space. (Gov't Exs. 70A-70G, 73A-73G).

5. Cell Phones

Two cell phones were seized and forensically extracted. One of the cell phones, a Samsung SM-G930V (the "new cell phone"), was the phone the Defendant was using. The second cell phone, a Samsung Galaxy 5G (the "old cell phone"), was not in use. The cell phones belonged to and were used by Defendant. Forensic data on the old cell phone showed that it has been used to access Pinterest on October 20 and 21, 2016. Images of nude females were found in the Pinterest cache. (Gov't Exs. 75B-F). Special Agent Debraux found these images were either "age difficult" (*i.e.*, it was not clear that the individual was a minor) or did not meet the federal definition for CSAM.

B. Defendant's Proof

1. Defendant's Testimony

Defendant Matthew Lynch testified on his own behalf. He declared that he is innocent of the charges. Specifically, Defendant stated that he has never looked at a pornographic image of person under the age of twelve or any pornographic images of children, has never received child pornography, and has never searched for child pornography online. He claims he does not know how the images were on his personal laptop. He stated that he did not use an external hard drive with his laptop, did not move files from his laptop to an external hard drive and had "no idea" how to do so, and did not know what a Seagate GoFlex hard drive looks like.

Defendant testified that he used FrostWire to download music and that sometimes the links did not provide content or returned jibberish. He testified that he primarily used Pinterest for nutrition and fitness information and that he had never seen the image of the three young girls until the search warrant execution (he claims he was shown an altered photo) or it was admitted as evidence at trial. When asked if he looked at adult pornography on Pinterest, Defendant responded that as far as he knew there was no pornography on Pinterest.

Defendant offered an explanation for his possession of the Maxtor hard drive and an alternative suspect – a childhood friend who allegedly used Defendant's family's computer (the one with the old Maxtor hard drive) in his parents' house in the early 2000s and also used Defendant's personal laptop computer between September 2016 and April 2017.

Defendant claimed that he did not know the Maxtor hard drive was in the storage tote found by investigators on April 11, 2017. Defendant stated that the Maxtor hard drive was from a family computer in the living room of his parents' house in the early 2000s. He explained that he got the tote from his parents' house when he was moving from Philadelphia, Pennsylvania, to Austin,

Texas, in 2015. During the move, he temporarily moved his things to his parents' house in trash bags. His parents were out of town at the time. He then dumped the contents of his trash bags into extra storage totes his mom had laying around without emptying the totes or checking their contents. He ended up using the red storage tote to store things in his closet, but claims he never looked through the tote or saw the Maxtor hard drive. Defendant said he did not realize it was in the tote until investigators found it.

Defendant also testified that there was one person other than himself who used his family computer in the early 2000s and his laptop in 2016/2017. That person was his childhood friend, Michael Evans. When Defendant mentioned Michael Evans, the Government said that it may need a recess to allow them to investigate this new evidence, perhaps to find Michael Evans and interview him. Defendant then disclosed that Michael Evans died of a drug overdose in 2019.

Defendant testified that after college, Michael Evans and other friends routinely visited Defendant's parents' house in Pennsylvania. The family computer was in the living room with the username and password taped to the monitor. Defendant testified Michael Evans used the computer, but he never saw him view CSAM on it.

Approximately fifteen years later, in September or October of 2016 through April 2017, Defendant claims Michael Evans stayed with him in his one-bedroom apartment in Nashville for unspecified blocks of time. Defendant testified that Evans had served time in jail, was struggling with drug addiction, and had used a debit card stolen from one of their friends to buy drugs. Nevertheless, because he wanted to help his old friend, Defendant let Evans stay in his apartment and gave him the password to his laptop. Defendant testified that Evans was staying in the apartment until April 10, 2017, the day before the search warrant was executed. Apparently in response to Detective Carrigan's testimony that the apartment was small, sparsely furnished, and

there was no evidence of another person living in the apartment, Defendant claimed that Michael Evans slept on a futon and had only a duffle bag and a backpack.

The Court observed Defendant's testimony and did not find it to be credible. His stories about the storage tote and the now-deceased friend are improbable and too convenient and well-crafted to be believable, and they cast a shadow over his credibility in general. While some aspects of the stories undoubtedly had elements of truth, Defendant's story appears carefully calculated not to contradict other evidence and, on the whole, the Court was left with the distinct impression that the tales were almost laughably incredible. In sum, Defendant appeared to be lying – not about everything, but about things that would be difficult to verify and things that seemed calculated to cast doubt on the Government's narrative. His story is simply not believable.

Other aspects of Defendants testimony also damage his credibility. For example, Defendant was evasive when asked if he used Pinterest to view adult pornography. Rather than answer yes or no, he said that he did not believe pornography was available on Pinterest. Not only was this answer evasive, but data from his cell phone indicates that he used Pinterest to view pornography. Similarly incredible, particularly considering that he worked for a computer company, is his testimony that he has no idea what a Seagate hard drive looks like and would have no idea how to move files from a laptop to a hard drive. To be sure, one would not be expected to know precisely what Seagate hard drive looks like, but to claim to have "no idea" is hyperbole that damaged Defendant's credibility.

Given the doubts as to Defendant's credibility and his incentive to lie, his denial of guilt is afforded no weight. Even so, the Government is held to its burden to prove the charges beyond a reasonable doubt.

2. Defense Expert

Michele Bush of Loehrs Forensics offered expert testimony on behalf of Defendant in the area of digital forensics. Bush has been a certified computer forensic examiner for over ten years. For the most part, Bush did not challenge the forensic extractions and analysis performed by Gish and Thomas. Except on one issue related to the Pinterest image, which is discussed in more detail below, the Court found her testimony credible.

At the outset, Bush identified perceived gaps in the Government's investigation – specifically, the failure to obtain search warrants for the contents of Defendant's Gmail and Pinterest accounts. She said the contents of these accounts would have provided valuable information. She was not aware that Pinterest and Gmail responded to record subpoenas, but said she would have liked to see information from the emails themselves, not just the account information.

As to the forensic evidence from the laptop, Bush stated that allocated files are not necessarily accessible to the average user. She agreed that the files in the FrostWire Siberian Mouse folder were accessible to the user at the time of the extraction, but said these were the only files an average user would have been able to access. She said it is possible a torrent search could return search results with links to illegal content, but agreed that the user would still have to select the link to download the content. She also agreed that the Siberian Mouse file name included abbreviations for terms indicative of child pornography.

Bush agreed that there was overwhelming evidence that a Seagate GoFlex hard drive that contained CSAM was plugged into the laptop between February 28, 2017, and April 9, 2017. She noted, however, that there was no evidence of ownership to attribute the Seagate hard drive to Defendant. One way to identify the user of a device is through personal files or accounts (email,

photos, resume, bills, etc.). Here, there was no forensic evidence that Defendant was, for example, using his email account while the Seagate hard drive was connected to his laptop, or evidence of identifying documents being moved to or from the Seagate hard drive. On cross examination, she acknowledged that because the Seagate hard drive has not been located, it was not possible to know the entire contents of the hard drive, only that personally identifying documents of the Defendant were not accessed from the Seagate hard drive while it was connected to the laptop.

With regard to the Maxtor hard drive, Bush did not dispute that the Maxtor hard drive contained thousands of CSAM images, but disagreed that the files were in allocated space. She noted that the Maxtor hard drive was originally part of a desktop computer that was used by Defendant and his father from 2000-2003 and then not accessed again until 2017 when it was forensically examined by investigators. Other than Defendant's father's use of the desktop computer containing the Maxtor, Bush did not identify forensic evidence of users other than Defendant for any of the devices.

Bush testified about the repinned Pinterest image, challenging the reliability of the image itself and the evidence that Defendant was the user who repinned it to his Pinterest account. She stated that she would expect to find forensic evidence of the Pinterest photo on the device used to repin the image, but no such evidence was found on the seized devices. She also stated that there is no conclusive evidence showing who was using Defendant's Pinterest account when the image was repinned, and no evidence connecting the Pinterest use to a specific device or specific user, only the IP address associated with Defendant's apartment.

As to the image itself, Bush questioned whether the image admitted during the trial as part of Government Exhibit 5, is the same image reported to NCMEC and provided to local law enforcement. According to Bush, the only way to be 100 percent certain that the images are the

identical is if the image has a hash value, which serves as a digital fingerprint. Here, the image did not have a hash value. Bush also suggested that the image she viewed at HIS was different than the one presented at trial. She testified that, according to the notes she took when she viewed the image at HSI in February 2023, the image showed the girls from the waist up. The image presented at trial which shows areas below the waist. On cross examination, the Government attorney asked her why she did not notice the alleged discrepancy when she viewed the image in 2023 given that the search warrant affidavit, which she said she had read, described the image as showing the girls' vaginas. Bush responded that this shows the importance of hash values and conceded that she did not compare the image she viewed at HSI to the description in the search warrant affidavit as closely as she should have.

Although the Court found Bush's testimony credible overall, her testimony that the image provided by HSI showed the girls only from the waist up appears have been a mistake. In any event, even without a hash value, the Court has no trouble concluding that the image reported by Pinterest, the image attached to the CyberTip, the image described by Detective Corrigan in the search warrant affidavit, and the image presented during the trial are the same. Bush's testimony does not raise reasonable doubt on this issue.

3. Character Witnesses

Defendant's childhood friends Patrick Walsh and Christopher Heron, and his co-worker and friend Caleb Johnson testified that Defendant has a reputation for truthfulness and honesty. Their testimony was credible. It does not, however, change the undersigned's opinion about the credibility of Defendant's testimony in this case.

IV. CONCLUSIONS OF LAW

A. Count One

Count One of the Superseding Indictment charges Defendant with violation of 18 U.S.C. § 2252(a)(2) which makes it unlawful to:

> knowingly receive[], or distribute[], any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if –
>
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (B) such visual depiction is of such conduct[.]

18 U.S.C. § 2252(a)(2). For the Court to find Defendant guilty of Count One, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant knowingly received a visual depiction.
2. That the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct.
3. That the visual depiction was of a minor engaging in sexually explicit conduct.
4. That the defendant knew that the visual depiction was of a minor engaging in sexually explicit conduct.
5. That the visual depiction was received using any means or facility of interstate commerce or by shipping or transporting in or affecting interstate commerce.

(*See* Joint Pretrial Brief (Doc. No. 97) (citing Sixth Circuit Criminal Pattern Jury Instruction 16.05).

The term "visual depiction" includes: data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a

visual image that has been transmitted by any means, whether or not stored in a permanent format. (*Id*.).

The term "minor" means any person under the age of 18 years. (*Id*.).

Sexually explicit conduct means (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; (v) lascivious exhibition of the anus, genitals, or pubic area of a person. (*Id*. (citing Sixth Circuit Criminal Pattern Jury Instruction 16.05 and 18 U.S.C. § 2256(2)(A)(5)). In deciding whether an exhibition is lascivious, the Court may consider: (1) whether the focal point of the visual depiction is on the child's genitalia or pubic area; (2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child; (4) whether the child is fully or partially clothed, or nude; (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer. (*Id*.); *see also*, *United States v. Brown*, 579 F.3d 672, 680 (6th Cir. 2009)) This list is not exhaustive, and an image need not satisfy any single factor to be deemed lascivious. Instead, the Court must determine whether the visual depiction is lascivious based on its overall content. (*Id.)*.

The term "in interstate commerce" means the visual depiction crossed a state line. The term "means or facility of interstate commerce" includes the internet. The phrase "affecting" interstate or foreign commerce means having at least a minimal effect upon interstate or foreign commerce. The government is not required to prove that the defendant knew that a means or facility of interstate commerce had been used when he received the images or that the defendant was involved

in any way in the production of the visual depiction. (*Id*.).

The Government introduced evidence that the Maxtor hard drive and Defendant's personal laptop contained images of minors engaged in sexually explicit conduct, and evidence that thousands of images were moved from Defendant's personal laptop to a Seagate external hard drive. To find Defendant guilty on Count One, the Government must establish the elements of the charge beyond a reasonable doubt with regard to at least one image. The Court focuses on three images on Defendant's personal laptop in the Frost Wire folder named *[April_2014][ALLTIMENUDES]1St Studio-Siberian Mouse-Nk007 Sample (Pthc 2012 Pedo).rar*.[3] These images depicted the following:

Government Exhibit 28 is a collage or image with many other images within it. Most of the images within the collage are of very young children engaging in sexually explicit conduct. The image in the bottom left corner is a photo with two little girls on a bed with teddy bears; their legs are spread apart, and their vaginas are exposed. The girls are prepubescent based on their body development (lack of body hair, breast development, hips). The image in the fourth row on the far left is a photo of a toddler girl; her legs are spread; her vagina is exposed; and someone is spreading her vagina apart.

Government Exhibit 30 is an image of a young girl who appears to be under the age of 18. Her vagina is exposed, and she is touching her vagina with an object.

---

[3] The Siberian Mouse folder contained two additional files: (1) an image of two girls kissing; they appear to be pre-teens or very young teens; their breasts are exposed (Gov't Ex. 29); and (2) an encrypted file named *1Studio – Siberian Mouse- Nk-007 Sample (Pthc 2012 Pedo).avi.* (Gov't Ex. 32). Investigators were unable to access the encrypted file. However, its name suggests it is a video featuring preteens engaged in sexually explicit conduct.

Government Exhibit 31 is a "contact sheet" showing thumbnail images of the contents of a compressed file. The underlying image and video files shown on the contact sheet were not present on the laptop. Some of these thumbnail images are of minors engaged in sexually explicit conduct. For example, an image showing the file name *[depa][boy+boy]depa01 2 12Yo Boys Suck Fuck Sound – Pedo G…* is of two young nude boys laying on a bed with their penises exposed.

Elements 2 and 3 are easily satisfied beyond a reasonable doubt. Having viewed Government Exhibits 28, 30, and 31, it is readily apparent that the images are of children under the age of 18 who are engaging in sexually explicit conduct. The production of the images necessarily involved the use of a minor engaging in sexually explicit conduct.

Element 5 is also easily met beyond a reasonable doubt because the images were torrent files downloaded from the internet. *United States v. Clark*, 24 F.4th 565, 573 (6th Cir. 2022) (citing *United States v. Pina*, 724 F. App'x 413, 422-23 (6th Cir. 2018) (holding that the internet is a means of interstate commerce).

Elements 1 and 4 require that the Defendant knowingly received a visual depiction and that he knew the visual depiction was of a minor engaging in sexually explicit conduct. The images were in allocated space and even Defendant's expert testified that these files were accessible to the user. The question is whether Defendant knowingly downloaded the files and knew the content of the files. In closing argument, counsel for Defendant argued the Government has not established this element beyond a reasonable doubt because someone other than Defendant could have downloaded the files to Defendant's personal laptop or Defendant could have downloaded the files by accident.

To show that the Siberian Mouse folder and its contents were knowingly on the laptop, Chad Gish explained that the process for downloading files using Frost Wire requires the user to

search for content and then click to download the specific file requested. Gish testified that Siberian Mouse is one of the most well-known series of CSAM. That, coupled with the fact that the Siberian Mouse folder title included the description "PTHC," which stands for "pre-teen hard core," and "pedo," leaves no reasonable doubt that the files were downloaded knowingly and not by accident, and that the user knew that the files contained images of minors engaging in sexually explicit conduct. In addition, there was evidence of thousands of other images of CSAM in the unallocated space of the laptop. The Government has proven beyond a reasonable doubt that images were knowingly received, and that the user knew the images were of minors engaging in sexually explicit conduct.

The final question is, "by whom?" Was Matthew Lynch the user who downloaded the CSAM content, or was it someone else? As evidence that Defendant was the user responsible for the content on the laptop, the Government presented evidence showing that the laptop belonged to Defendant, that it was password protected, that the only user account was Defendant's, and that there was no forensic evidence of another user of the laptop.

Defendant professed his innocence and testified that a childhood friend, who is now deceased, had access to his laptop in 2016/2017 and to the Maxtor hard drive in 2001/2002 and could have downloaded the CSAM images on his laptop and transferred images to the Seagate external hard drive. The defense argues that the timeline related to the Seagate hard drive – that it was connected to the laptop only between February 28, 2017, and April 9, 2017 – suggests someone other than Defendant connected it to the laptop and raises reasonable doubt as to Defendant's culpability.

The Court disagrees. Defendant's hypothesis that his friend could have been responsible for downloading the Siberian Mouse files from Frost Wire and transferring files to the Seagate

hard drive does not raise a reasonable doubt that someone other than Defendant was responsible. As explained above, the Court does not find Defendant's testimony, which is not supported by any corroborating evidence, credible. Considering the totality of the evidence, the Court finds that the Government has proved elements 1 and 4 beyond a reasonable doubt – Defendant knowingly received a visual depiction and that he knew the visual depiction was of a minor engaging in sexually explicit conduct.

Accordingly, the Court finds the Government has proved each of the elements beyond a reasonable doubt. Accordingly, Defendant is adjudged GUILTY of the charge in Count One of the Superseding Indictment.

B. Count Two

Count Two charges Defendant with violation of 18 U.S.C. § 2252(a)(4)(B), which makes it unlawful to:

> knowingly possess[], or knowingly access[] with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if –
>
> (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (ii) such visual depiction is of such conduct[.]

18 U.S.C. § 2252(a)(4)(B). Count Two further charges that the visual depiction involved the use a prepubescent minor or a minor who had not attained twelve years of age. For the Court to find Defendant guilty of Count Two of the Superseding Indictment, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant knowingly possessed or accessed with intent to view one or more matters containing a visual depiction.

2. That the production of the visual depiction involved the use of a minor who had engaging in sexually explicit conduct.

3. That the visual depiction was of a minor engaging in sexually explicit conduct.

4. That the defendant knew that the visual depiction was of a minor engaging in sexually explicit conduct.

5. That the visual depiction had been shipped or transported using any means or facility of interstate commerce or in or affecting interstate commerce.

(*See* Joint Pretrial Brief, Doc. No. 97 (citing Sixth Cir. Pattern Criminal Jury Instruction 16.06; 18 U.S.C. § 2252A(a)(5); 18 U.S.C. § 2252(a)(4)(B)).

The terms "visual depiction," "minor," and "sexually explicit conduct" have the same definitions as relevant to Count One. (*Id*.). The terms "in interstate commerce," "means or facility of interstate commerce," and "affecting interstate commerce," also have the same meaning as provided with regard to Count One. (*Id*.). As with Count One, the Government does not have to prove that the Defendant was involved in the production of the visual depiction. (*Id*.). The Government also does not have to prove that Defendant viewed the images or that his individual conduct substantially affected interstate commerce. (*Id*.).

The Court begins with elements two through five. Here the conduct at issue is Defendant's alleged repin of an image on Pinterest. The image in question was attached to Pinterest's report to NCMEC.[4] The image is of three young girls sticking out their tongues and pinching their nipples.

[4] Defendant argues that the Government has not shown beyond a reasonable doubt that the image Pinterest submitted to NCMEC, the image provided to law enforcement, and the image admitted as evidence at trial (Gov't Ex. 5) are identical because the image does not have a hash value. The lack of a hash value does not raise reasonable doubt that the images are the same, particularly where the description of image provided to law enforcement as described in the search warrant affidavit matches the image admitted into evidence during the trial and there is no persuasive evidence that the images are not the same.

The photo shows the genitals or pubic area of the girls. A pink object that appears to be a toy is partially covering the pubic area of one of the girls.

The Court finds this image depicts sexually explicit conduct in that it is a lascivious exhibition of the genitals or pubic area of the children pictured. In reaching this conclusion the Court has considered the six factors set forth in *United States v. Brown*, 579 F.3d 672, 680 (6th Cir. 2009). Here the following factors and the overall content of the image point toward a finding of lasciviousness: (1) the children are entirely nude; (2) the children are depicted in an unnatural pose, pinching their nipples and sticking out their tongues; (3) one of the children has a toy or object on her vagina; (4) the image appears designed to elicit a sexual response in the viewer. *See id.*; *see also United States v. Daniels*, 653 F.3d 399, 407 (6th Cir. 2011).

The size and body development of the girls indicates that they are minors; at least two of the girls are prepubescent and under the age of twelve. The girls have minimal breast development and no pubic hair. Because their young age is readily apparent, the Court has no trouble finding beyond a reasonable doubt that the viewer knew the children were minors and that at least two of them were under the age of twelve. Therefore, the third and fourth elements are satisfied. The second element is also satisfied because the minors who are the subject of the image were necessarily involved in its production while engaging in sexually explicit conduct.

The fifth element – that the visual depiction had been shipped or transported using any means or facility of interstate commerce or in or affecting interstate commerce – is easily satisfied beyond a reasonable doubt because the image was accessed via the Pinterest phone application and the internet. *United States v. Clark*, 24 F.4th 565, 573 (6th Cir. 2022) (citing *United States v. Pina*, 724 F. App'x 413, 422-23 (6th Cir. 2018) (holding that the internet is a means of interstate commerce).

The first element – that the Defendant knowingly possessed or accessed with intent to view one or more matters containing the visual depiction – is the most contentious. Put simply, the question is whether Defendant was the user who repinned the image to his Pinterest board and whether he did so knowingly.

The evidence shows that, on October 24, 2016, Defendant logged into his Pinterest account from an Android device using the IP address associated with his AT&T U-verse account for his apartment on October 24, 2016. (*See* Gov't Exs. 1, 3, 5). Both of the cell phones recovered were Android devices. Defendant's Pinterest account was a verified account, meaning Pinterest sent an email to his email address and he responded to that email confirming the account registration. Furthermore, Defendant told Detective Carrigan that he had a Pinterest account and that he had been locked out of Pinterest more than once. From the same IP address, on October 29, 2016, Defendant repinned the image through "IN_APP_BROWSER," meaning the user "clicked through a Pin to view the original website, then pinned the image from within the browser preview." (*See* Gov't Ex. 5, Def. Ex. 8). The image was repinned using a multi-step process, removing any reasonable doubt that the repin was done knowingly.

In sum, the Government has proven beyond a reasonable doubt that Defendant was the user who repinned the image to his Pinterest board and that he did so knowingly – i.e., he knowingly accessed with intent to view and did, in fact, view the image. Element one is, therefore, satisfied.

For the reasons stated, the Court finds the Government has proved each of the elements beyond a reasonable doubt. The Court specifically finds that the visual depiction involved the use of a prepubescent minor or a minor who had not yet attained twelve years of age engaged in sexually explicit conduct and that the visual depiction was of such conduct. Accordingly, Defendant is adjudged GUILTY of the charge in Count Two of the Superseding Indictment.

It is so **ORDERED**.

WILLIAM L. CAMPBELL, JR.
CHIEF UNITED STATES DISTRICT JUDGE